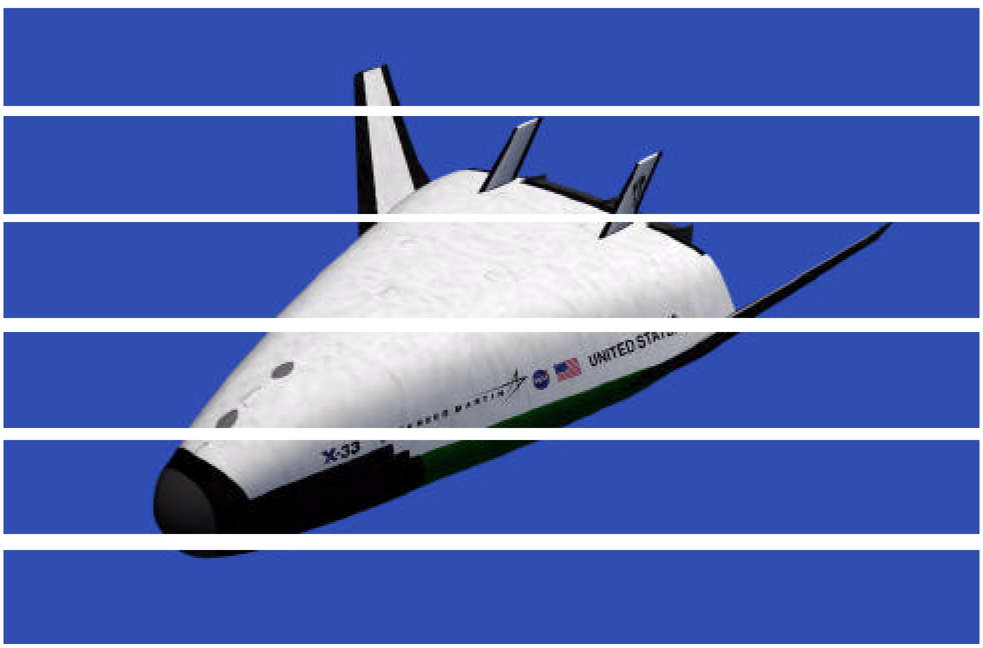
X^{33}

Safety & Mission Assurance Review



NASA Office of Safety & Mission Assurance

March 5, 1998

306-F

Executive Summary

The X-33 Program safety, risk management, and mission assurance management processes were reviewed by the NASA headquarters Office of Safety and Mission Assurance (OSMA) during February 1998. An OSMA review team conducted on-site reviews at the Lockheed Martin Skunk Works (LMSW) facility in Palmdale, California, on February 19 and 20. The OSMA review team examined findings of previous X-33 reviews (Non-Advocate and Independent Annual Reviews), and numerous X-33 program documents related to safety and mission assurance. This research was supplemented by pre-meeting telephone discussions with NASA and LMSW personnel and the on-site review.

The review team observed that NASA Safety and Mission Assurance (SMA) visibility into the X-33 program, as well as the X-34 program and other "Faster/Better/Cheaper" NASA initiatives, must be restored to a level of involvement consistent with an "insight" role. NASA cannot exercise top-level risk management responsibilities for public safety, financial resources, and liability without an appropriately defined, funded, and staffed SMA role. The review team recommends the immediate establishment and implementation of an X-33 program funded, Marshall Space Flight Center (MSFC) SMA managed, "X-33 Safety & Mission Assurance Program." This action needs to be taken prior to NASA assuming any additional liability for mishaps, an action that is currently proposed in the amendment to the Space Act to indemnify X-programs against liability. This revised SMA role must also be reflected in the Program Commitment Agreement revision, currently in-work by X-33 program management, with specific reference to NASA's role in signing the Certificate of Flight Readiness (COFR).

The review team found evidence that rigorous safety, mission assurance, and risk management processes were being employed by the LMSW throughout the X-33 program. A number of minor concerns are highlighted in the report. The review team identified a number of areas which will require increased NASA Safety & Mission Assurance (SMA) involvement in order to achieve a level of insight consistent with overarching NASA responsibilities. Included are issues related to safety of flight, flight termination system redundancy, and other areas with potential impact on the general public. The review team also noted a number of high-risk programmatic or mission assurance concerns which have the potential of becoming safety issues.

Expanding SMA insight and participation in the X-33 program will enhance the likelihood of mission success and provide assurance that risks to public safety have been appropriately addressed. The increase in SMA insight will also provide the depth of understanding and level of confidence necessary for NASA to support X-33 launch, and flight operations.

Table of Contents

1.0 Introduction

A review of the X-33 was conducted by the Associate Administrator for Safety and Mission Assurance in coordination with the Associate Administrator for Aeronautics. The purpose of this review was to establish a better understanding of the X-33 risk management approach and the safety and mission assurance processes which are being implemented to assure safety of flight and mission success.

The following paragraphs, abstracted from the letter initiating the study, describe key considerations and provide overall context for this review:

> *NASA is ultimately accountable and liable to Congress and the American people for the safe and successful conduct of all NASA programs. There is a shared responsibility between NASA and its industry contractors to assure that programs are conducted safely and successfully.*
>
> *Specifically, NASA program managers are: "responsible for the safety and mission success of their programs."*
>
> *The SMA function, at the Centers and at Headquarters, has the responsibility for: "ensuring that effective and efficient SMA functional management is in place to enhance the potential for success of NASA programs," and for "ensuring oversight and independent assessments to ascertain that appropriate risk management practices are used for the identification, documentation, evaluation, and disposition of all SRM&QA risks for all programs, projects and operations."*
>
> *To allow us to implement and fulfill the NASA SMA policies, we are suggesting the enclosed agenda. It is vitally important that the X-33 program understand that we are not asking for a dedicated safety review, presented by X-33 staff having responsibility for flight assurance. Rather, we are interested in gaining a complete understanding of the X-33 risk management processes and the safety and mission assurance processes which are being implemented to assure safety of flight and mission success.*

The Program Office at Lockheed Martin SkunkWorks (LMSW) in Palmdale, California, was tasked to present a top level discussion of X-33 management, engineering, and mission assurance processes which address overall safety, schedule, budget, and programmatic risk issues. The review team was led by Mr. Frederick D. Gregory, Associate Administrator for Safety and Mission Assurance, and was supported by members of his staff from the Enterprise Safety and Mission Assurance Division and the Safety and Risk Management Division.

Members from the NASA Aerospace Safety Advisory Panel were also present and participated in the review.

2.0 Background

2.1 Concept

The X-33 Program will demonstrate the key design and operational aspects of a Single Stage to Orbit (SSTO) Reusable Launch Vehicle (RLV) rocket system to reduce the risk to the private sector in developing such a commercially viable system. The X-33 program will implement the National Space Transportation Policy, specifically Section III paragraph 2(a), which states: "The objective of NASA's technology development and demonstration effort is to support government and private sector decisions by the end of this decade on development of an operational next-generation reusable launch system."

This is being accomplished through a three-phase program. Phase I, which has been completed, was a 15-month competitive demonstration of critical technologies and included development of program plans for ground and flight demonstrations to be executed in Phase II. LMSW was selected as the single industry team to continue into Phase II. The next major decision point will be at the end of X-33 flight and ground tests when the government and industry will decide whether to enter Phase III, the development of the full-scale operational RLV.

The X-33 Advanced Technology Demonstrator represents a 53-percent scale model of the future Lockheed Martin Reusable Launch Vehicle, VentureStar. Through the Phase II ground and flight demonstrations, the X-33 will provide information necessary to allow the government-industry team to make a decision on whether to proceed in the development of the full-scale, commercial , single-stage-to-orbit RLV. If developed, the VentureStar would eventually replace the Space Shuttle as the next generation space transportation system. The goal is to lower costs from approximately $10,000 per pound down to near $1,000 per pound to low earth orbit.

2.2 Cooperative Agreement

The X-33 Program is established as a Cooperative Agreement between NASA and LMSW. The X-33 is an industry-led program with NASA assuming an insight rather than the conventional oversight role. The responsibility for determining how the program will be implemented and the accountability for meeting program milestones resides with the industry partner. Industry has complete design authority for both the X-33 and the operational RLV.

One of the unique features of the cooperative agreement is that NASA Centers support the industry team through task agreements that are negotiated between LMSW and the individual NASA Centers. These task agreements define NASA’s products, delivery schedule, and facility requirements. There are currently over one hundred task agreements involving all ten

NASA Centers. Additionally there are DOD task agreements involving the Air Force Flight Test Center, Michael Army Air Field, Malmstrom AFB, and Wright Aeronautical Laboratory.

2.3 Liability and Indemnification

Issues of liability and indemnification are described in Section 33 of the Cooperative Agreement:

> "The parties recognize that potential liability to third parties is a substantial concern against which the Recipient (Lockheed Martin) desires indemnification by NASA. If legislation is enacted which provides NASA specific authority, NASA agrees to process the Recipient's application to indemnify Recipient against claims of third parties for death, bodily injury, or loss of, or damage to, property resulting from flight testing of the X-33 vehicle in the performance of this cooperative agreement. In the event that indemnification is not provided, either because legislation is not enacted or because an application for indemnification submitted by the Recipient is disapproved for good reasons, the recipient shall be responsible, either through insurance or otherwise, for any third-party liability it may incur under this agreement. In this event the parties will include in their financial contribution the cost of insurance or take other measures to provide for the financial protection against third-party liability."

Under pending legislation (Senate Bill 2150), indemnification or partial indemnification would be granted. However this legislation also states that: "The Administrator may not provide liability insurance or indemnification unless the developer establishes to the satisfaction of the Administrator that appropriate safety procedures and practices are being followed in the development of the experimental aerospace vehicle." This would suggest that NASA, as the government partner, must assume a more traditional oversight role with respect to the safety and mission assurance function if indemnification is granted.

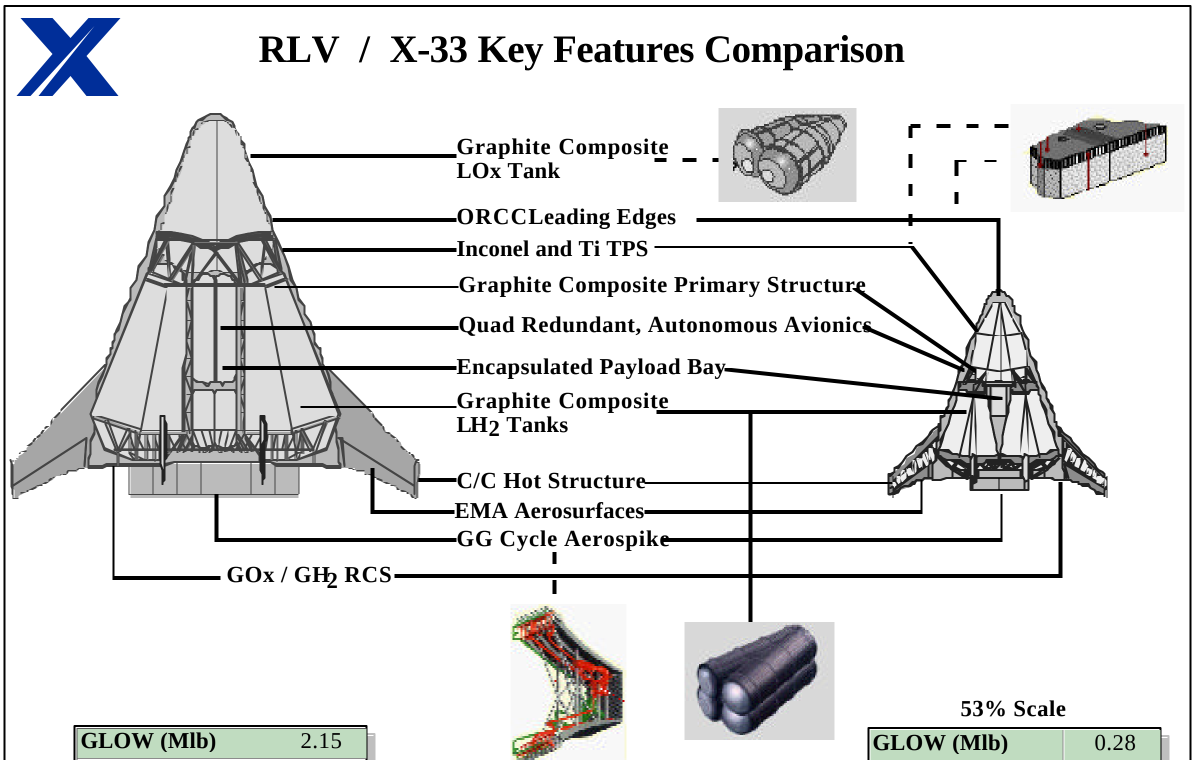
No cross waiver authority exists under the current Cooperative Agreement. Cross waiver authority allows each party to bear its own risks i.e. the involved parties agree not to bring suit against each other. Further, the pending legislation does not include cross waiver authority.

2.4 Range/Facilities

The Air Force Flight Test Center (AFFTC) at Edwards Air Force Base (EAFB) has been selected to be the X-33 launch site because proximity to LMSW and the availability of a sparsely populated launch corridor for launches toward the northeast. The X-33 will be launched from the site near Haystack Butte, located at the eastern edge of EAFB. Landing sites include Michael Army Air Field at Dugway Proving Ground in Utah and Malmstrom Air Force Base near Great Falls, Montana. The X-33 will be returned to the launch site using a specially designed ground transportation system. Initially the X-33 was to have been ferried back to the launch site via the Shuttle Carrier Aircraft (SCA) now used to ferry the Space Shuttle across country. Approximately 100 workers will construct the $30 million launch facility, with work scheduled to be completed in a year. Sverdrup Corporation, St. Louis, MO, is overseeing construction of the facility. Site plans include a retractable vehicle shelter; a rotating vehicle launch mount; storage areas for the liquid hydrogen and liquid oxygen propellants, and helium and liquid nitrogen used in vehicle operations; a water storage tank for the sound suppression system; a concrete flame trench; and assorted site infrastructure. The vehicle's operations control center will be located in an existing test control room within Haystack Butte.

2.5 Vehicle Manufacturing

Construction has begun on the X-33 and major components are already taking shape. The large aluminum tank that will contain the liquid oxygen has been completed and was recently delivered to the LMSW. The final assembly jigs are already in place at the LMSW facility at Palmdale. Figure 2.1 presents a comparison between key structural and propulsion elements of the X-33 and RLV.



GLOW (Mlb)	2.15
Dry Weight (Klb)	197
Mass Fraction	0.91
Length (ft)	127
Velocity	Orbital

GLOW (Mlb)	0.28
Dry Weight (Klb)	63
Mass Fraction	0.77
Length (ft)	63
Velocity	Ma 15

Figure 2.1

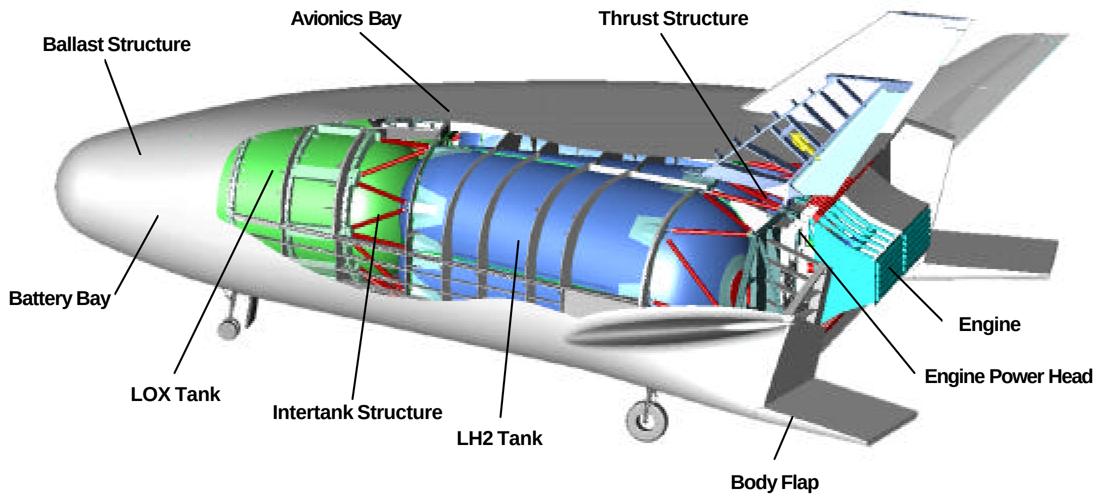


Figure 2.2

Figure 2.2, provides a cutaway view of the X-33, showing the location of LOX and LH2 tanks and indicating thrust load paths through the tanks and intertank structures.

2.6 Schedule

The projected date for the X-33 rollout is May 1999, with its first flight currently planned for July 27, 1999. The program is scheduled to be completed by 2000.

2.7 Operations

The X-33 Advanced Technology Demonstrator is an unmanned, autonomous vehicle that uses differential Global Positioning System (GPS) with a radar altimeter for navigation and landing. The differential GPS will guide it through its flight and down the runway for landing. The X-33 will operate as an autonomous vehicle during normal operations. The uplink to the X-33 would only be used if the vehicle deviates significantly from its planned flight path. The X-33 preflight and flight operations will be monitored and controlled from a refurbished operations control center located in Haystack Butte. At the Michael AAF and Malmstrom AFB landing sites there will be a back-up Mobil Operations Control Center only. There will also be range safety officers at the downrange sites. The X-33 is designed to reach Mach 12.6; the current flight test plan specifies a maximum velocity of Mach 12.6 for flight tests to Malmstrom AFB. The X-33 is not designed for, nor intended to, achieve orbital velocities (which would require a speed of more than Mach 25).

2.8 Launch Readiness Test

Once the X-33 is readied for flight, the engines will undergo two flight readiness firing tests on the launch pad. The purpose of these tests is to validate lift-off acoustic and over-pressure environments and confirm integrated main propulsion performance.

2.9 Flight Test Program

No more than 15 flights are currently planned for the X-33 from the EAFB launch site at Haystack Butte. The X-33 Team has defined a series of seven flights that will, if successful, satisfy all program objectives and provide the data needed to establish the confidence for a decision to proceed with the full scale VentureStar. Flights 1-5 will be to Michael Army Air Field (AAF) and will investigate aero plume and shock-shock interactions, boundary layer transition, thermal protection system (TPS) panel thermal properties, real gas effects, and thrust vector control. Flights 6 and 7 will be to Malmstrom Air Force Base (AFB) and provide additional data on real gas effects. Flights 8 to 15 are to provide additional margin to accommodate test objectives not accomplished in Flights 1-7.

<u>X-33 Flight Test Plan</u>

Test flights involve:

(1) launching the X-33 from a vertical position like a conventional space launch vehicle - to reduce the structural requirement and weight of the landing gear and wheels to that required to support an unfueled vehicle. The baseline dry weight of the X-33 is approximately 75,000 lb. and fueled weight of is approximately 123,800 kg (273,000 lb);

(2) accelerating the vehicle to top speeds of Mach 12.6 (12.6 times the speed of sound) or approximately 18,000 km/hr (11,000 mph) and reaching altitudes up to approximately 75,800 m (250,000 ft);

(3) shutting down the engines and gliding over long distances, up to 1,530 km (950 mi) downrange of the launch site, followed by conducting terminal area energy maneuvers to reduce speed and altitude; and

(4) landing like a conventional airplane.

The original flight test plan included three short-range, seven mid-range, and five long-range test flights. Using a launch and flight operations site at EAFB, remote landing sites were selected which would accommodate incremental advances to Mach 4, 9, and 15 for the baseline vehicle (Figure 2-3). This would involve flights of approximately 160, 720, or 1,530 km (100, 450, and

950 mi). Actual numbers of test flights to any range would vary due to changing plans and/or actual test flight data evaluation.

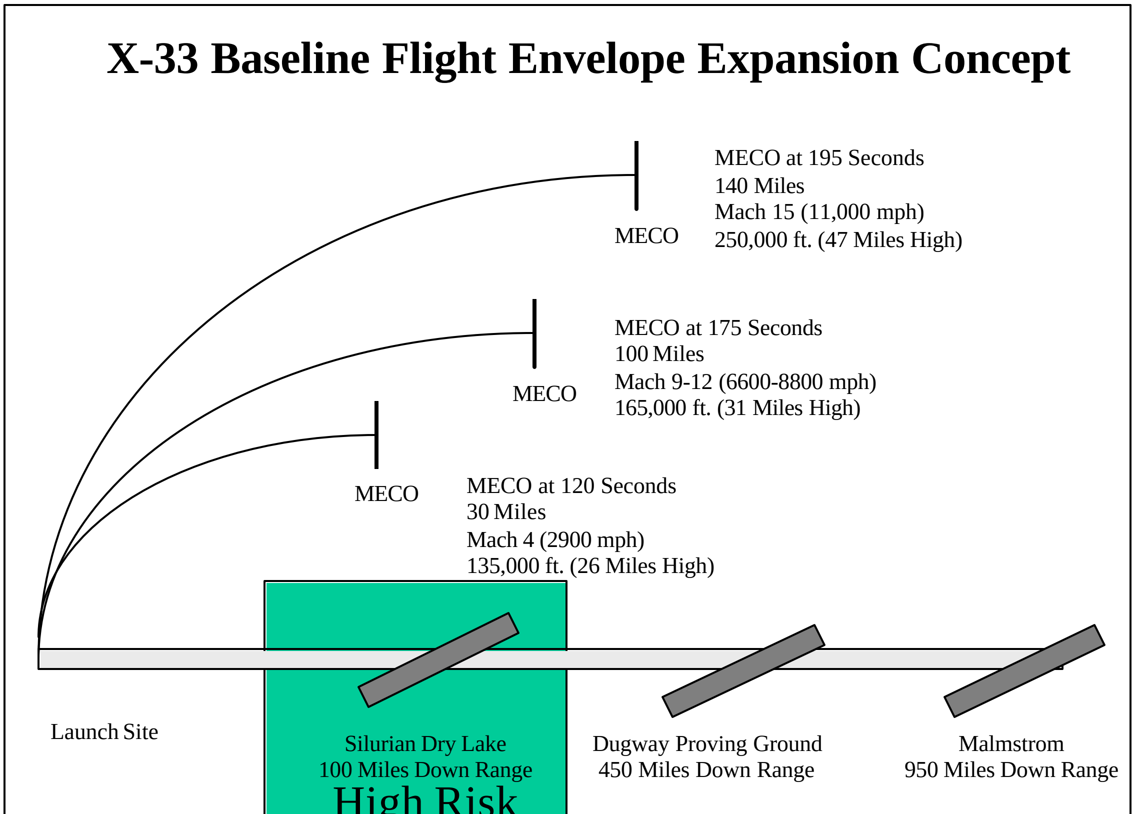


Figure 2-3

<u>Short Range Destination: Silurian Lake, California</u>
(Now eliminated from the flight test program. See discussion under Mission Assurance, Section 5, of this report.)

The U.S. Department of the Interior, Bureau of Land Management (BLM), is the federal government manager of the property and much of the surrounding area. (A pending future action involves transferring this property to the U. S. Army, Ft. Irwin, California, for expansion of their boundaries and capabilities in desert warfare training.) Silurian Lake is classified by BLM as a Multiple Use I (intensive use) area and such activities as commercial filming have been permitted at the site.

<u>Medium Range Destination: Michael Army Airfield on Dugway Proving Ground, Utah</u>

Dugway Proving Ground is located approximately 130 km (80 mi) southwest of Salt Lake City, Utah, near the town of Tooele. Dugway Proving Ground encompasses approximately 324,000 ha (800,000 ac) of the Great Salt Lake Desert. Dugway is part of the U.S. Army Test and Evaluation Command, headquartered at Aberdeen Proving Ground, Maryland.

The airfield within Dugway Proving Ground proposed for landing the X-33 is called Michael Army Airfield. This airfield is located on the eastern boundary of Dugway. The airfield has a 3,960 m (13,000 ft) long by 61 m (200 ft) wide hard surfaced runway. Immediate surrounding terrain is relatively flat. It is a secure facility with a long history of flight operations. The airspace above Dugway Proving Ground is restricted military airspace controlled by Hill Air Force Base which manages and approves use of the Utah Test and Training Range (UTTR).

Dugway is primarily responsible for planning, conducting, and analyzing tests involving chemical warfare and biological defense systems; flame, incendiary, and smoke obscurant systems; and artillery systems to determine their applicability to military defense programs. The Air Force manages the UTTR at Michael Army Airfield on Dugway. Their primary mission is testing and evaluating unpiloted aerospace vehicles (UAV's) and UAV launch and recovery systems. They support testing of weapons systems; training for operational aircrews and other combat units; maintaining and operating a variety of aircraft; scheduling and monitoring flight activities; and providing range support and air traffic control. UTTR operations are compatible with the mission of the X-33 Program. New site preparation will primarily involve runway lengthening and widening.

<u>Long Range Destination: Malmstrom Air Force Base, Montana</u>

Malmstrom Air Force Base is located 12 km (7 mi) east of downtown Great Falls, Montana. The installation occupies approximately 1,279 ha (3,159 ac). It is home to the 341st Missile Wing (341 MW), which is responsible for operation, maintenance, and security of assigned intercontinental ballistic missile systems. Since the late 1980's, Malmstrom Air Force Base has been home to the 43rd Air Refueling Group. As a result of the Department of Defense's Base Realignment and Closure Plan, the 43rd Air Refueling Group was transferred to MacDill Air Force Base, Florida. After the move, the airfield was closed on December 31, 1996, except for the area used by helicopters of the Malmstrom's Air Rescue Flight. The airfield has a hard surface runway approximately 3,500 m (11,500 ft) long and 61 m (200 ft) wide with a 305 m (1,000 ft) overrun at each end. Since the closure of the airfield, the USAF has no plans or budget to operate the runway. There is no control tower, no instrument landing system, no visual aids for visual approach, no slope indicator lights, no airfield weather support, and no on-going maintenance of the runway. The terrain surrounding the airfield is relatively flat. At the time of the proposed X-33 flights, the airspace will be under Federal Aviation Administration (FAA) control. Reopening of the airfield through permission of the USAF and/or Congressional authorization would be required in order for NASA to land the X-33 at this facility, even on a limited, temporary basis. Discussions with LMSW indicate that this administrative process has been completed.

2.10 Technology Demonstration Objectives

The X-33 is expected to demonstrate new technologies which include the linear aerospike engine, a large composite liquid hydrogen tank, the spacecraft's lifting body design, vehicle reusability, i.e., a reusable TPS, and autonomous operations. A key program objective is to demonstrate a two-day turnaround for the vehicle for any one flight and a seven day turnaround for three consecutive flights.

The engine is designed to provide high performance over a broad range of altitudes and is believed to be more efficient and a better fit for the wedged-shaped aircraft than conventional bell nozzle rocket engines. Demonstration of actual flight performance of the linear aerospike engine integrated with the lifting body represents one of the most challenging and critically important technical objectives of the X-33 program.

The X-33 flight system, subsystems, and major components are to be designed and tested (in flight and ground) so as to ensure their traceability (technology and general design similarity) and scaleability (directly scaleable weights, margins, loads, design, fabrication methods, and testing approaches) to a full scale single-stage-to-orbit (SSTO) launch system. Technical objectives also include improved mass fraction for vehicle structures.

The X-33 Advanced Technology Demonstrator is intended to demonstrate key "aircraft like" operational attributes required for a cost effective SSTO launch system. At a minimum, key demonstrations will include: operability (e.g., increased TPS robustness, weather, etc.), reusability, affordability, and safe abort.

3.0 Safety & Mission Assurance Processes

3.1 Overview

The LMSW has implemented numerous interlocking and overlapping processes which are capable of effectively managing programmatic and safety risks in the X-33 program. The LMSW SMA process is comprised of three fundamental building blocks: Systems Engineering, Flight Assurance, and the Chief Engineer.

<u>Systems Engineering</u>

Systems Engineering is responsible for: Configuration Management, Risk Management, and Certification Compliance.

- Configuration Management provides the program-wide configuration management function.
- Risk Management provides the integrated management of Risk Management planning, documentation, tracking, and close-out of open items. *(An expanded discussion of the Risk Management activity is provided later in this section.)*
- Certification Compliance provides continual documentation of X-33 compliance with program requirements.

<u>Flight Assurance</u>

Flight Assurance is responsible for: Systems Safety, Quality Assurance, Flight Test, Systems Assurance, and Systems Integration.

- The Systems Assurance function includes: Range Safety, Range Management, Environmental and Special Analysis. *(Range Safety is discussed at greater length later in this section.)*
- The System Safety function performs Hazards Analyses. (*The Hazard Analysis process is examined, later in this section.)*

<u>Chief Engineer</u>

The Chief Engineer is responsible for a variety of activities including the Operations group and Systems Operations group, which chairs the Engineering Review Board Process.

- Within the Operations group one finds the Maintainability and Supportability division which develops; Fault Tree Analyses, Failure Modes and Effects Analyses, and the Critical Item List (CIL) (*discussed later in this section.).*

Program Boards and Risk Management Interactions

The highest level risk management tool is the formal program-level risk management process. The risk management process identifies, evaluates, quantifies, and tracks any open or unresolved risk (safety and/or programmatic) issue which has cost or schedule implications. Examples include: vehicle weight growth, successful completion of the Environmental Impact Assessment process, acquisition of liability indemnification, Liquid Hydrogen Tank manufacturing issues, and Flight Termination System (FTS) redundancy. Safety issues will appear on the top-level risk management "radar screen" if they are not satisfactorily addressed in other engineering or safety specific risk management forums, such as the Engineering Review Board and the Systems Safety Review Board. Each of the discipline-specific risk management activities are self contained risk management processes possessing the basic risk management attributes of risk identification, risk evaluation, risk mitigation/acceptance, and risk tracking and documentation. As Shown in Figure 3-1, the Systems Engineering, Risk Management Board is the highest level management forum. Next level down is the Engineering Review Board (ERB) which reviews change requests to the program baseline. Flight Assurance, including Systems Safety, flows into the ERB forum.

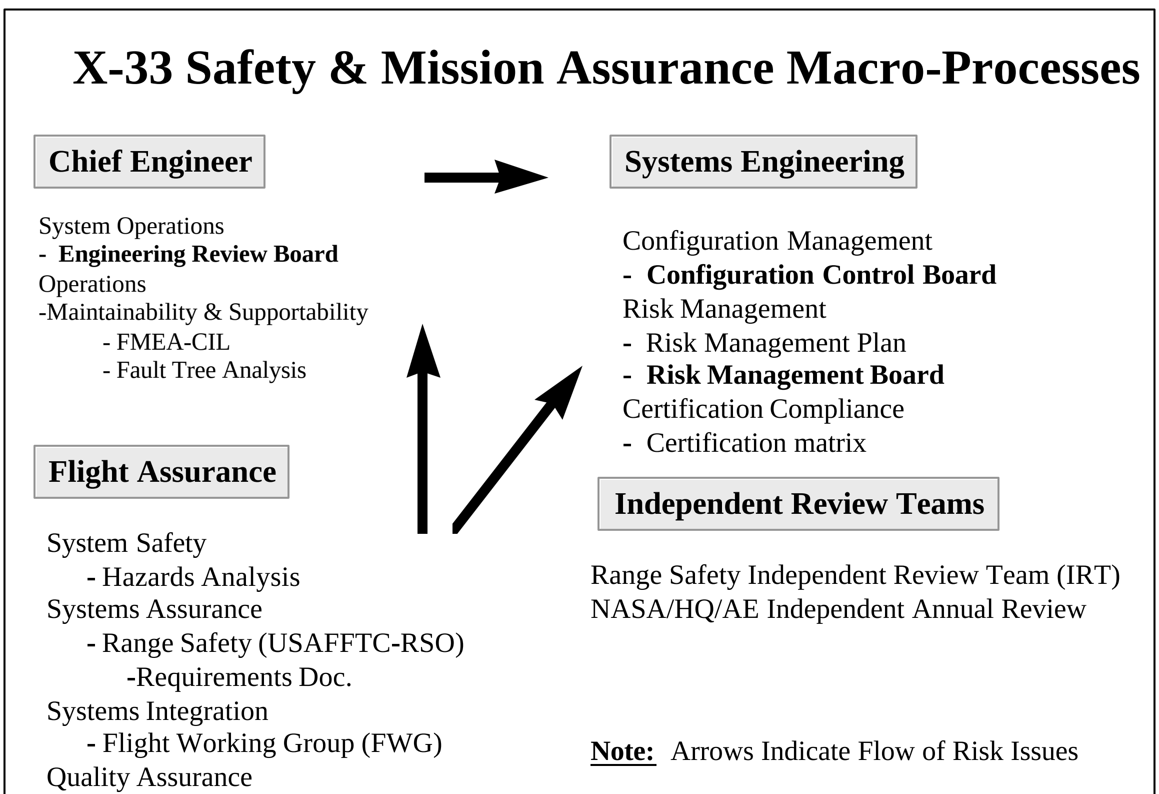


Figure 3-1

An expanded discussion of selected safety and mission assurance processes and the implementation of risk management tools and techniques is provided in the following sections.

3.2 Risk Management Process

Risk Management Plan Assessment

Overall, the X-33 Risk Management Plan is impressive. There is certainly evidence of a comprehensive risk management process that has been in existence for some time (at least back to 1996). The steps in their process are: Identification, Quantification, Mitigation (Planning / Implementation), Execution, and Tracking. These steps are similar to the steps which we would consider to constitute a good risk management process. The X-33 project appears to have a good risk management organizational structure, including a Risk Management Board that meets monthly to assess and prioritize risks and approve and review the status of risk mitigation plans. The project has identified a significant number of X-33 risks and ranked them based on estimated (qualitative) probability and consequences. (In the material sent to the review team, there were 27 risks rated high or medium; the total number of risks is approximately 1100).

The project's descriptions of the identified risks are somewhat lacking—they tend to state the condition that is of concern for each risk but usually do not clearly state what the undesired consequence might be. Also, there is not enough information in the risk management plan to determine exactly how they assign values between 0 and 1 to probability and consequence, but this is being done successfully, presumably detailed guidance exists elsewhere.

The X-33 program concentrates its risk management efforts on the high and medium risks. They have a risk tracking form which leads to risks being entered into a database. There is a risk database containing all of the identified risks (some of which have been closed in the past, accounting for the gaps in the risk numbering). In addition to high and medium risks in the database, they also maintain records of low risks. Some risks do not have ratings in the database. The review team assumes that none of the unrated risks are actually high or medium. Safety is not among the areas explicitly addressed in the X-33 Risk Management Plan or process. Safety risks are, for the most part, handled separately in a parallel process. Only when a particular safety risk might compromise program success does it become a member of the program’s list of top risks. It would be somewhat more satisfying if safety risks were included under the risk management umbrella (NASA’s risk management process explicitly includes safety risks along with the other types), but the program has chosen to handle them separately and this arrangement appears to be working well.

The X-33 project tracks risks for changes over time, i.e., "waterfall" trend charts as well as status reports in the database. Risks are periodically reviewed as evidenced by a September 1996 status report and a December 1997 Quarterly Status report. Risks are reviewed monthly.

There is evidence in the database of mitigation planning and follow-up on many of the high and medium risks.

3.3 Hazard Analysis

The Hazard Analysis process has identified more than 1700 separate safety hazards. The self-contained Hazard Analysis System, supported by Failure Modes and Effects Analysis and Fault Tree Analysis activities identifies, evaluates, and mitigates safety risks. Safety risks are addressed in the Systems Safety Review Board management forum. It is the intent of the X-33 program to eliminate or mitigate all documented risks prior to the first flight. It was stated that 90 days prior to launch all hazards will be reviewed. All hazards will be closed out before flight.

3.4 Failure Modes and Effects Analysis (FMEA) Process

The X-33 program has implemented a rigorous use of the FMEA methodology in identifying and controlling risk. Potential weaknesses include the use of multiple formats in characterizing failure effects and inconsistency in the degree to which end-effects were estimated. A large number of Category 1E (critical but low probability) failure modes exist as shown in Figure 3.2 below.

Closed-Loop Failure Mitigation in Design and Manufacturing Processes

Critical Items List based on FMECA

Hazard Severity / Prob. of Occurrence	CAT I Loss of Vehicle/Death	CAT II Damage to Vehicle/Injury	CAT III Impact to Mission	CAT IV Negligible
(A) Frequent				1
(B) Probable				
(C) Occasional		2		8
(D) Remote	43	88	478	1391
(E) Improbable	1089	453	1906	1664

CIL — Corrective / control actions must be taken

Remaining Blocks Not critical to Reliability program

Failure Mitigation Customized by LRU:

- Qualification Tests / Analyses match predicted environment
- OEM Inspections and Functional Testing
- Environmental Stress Screening
- System Checkouts @ Palmdale & EAFB
- Maintenance per tailored RCM process
- etc.

Avionics Environmental Stress Screening (ESS)

- Vibration - 3 Axes
- 10 Thermal Cycles
- Functional Test
- Min. 3 Failure Free Cycles

Notes: *(1) P(Occurence) considers redundancy. (2) Counts reflect component failure modes (LRUs can have multiple crit modes). (3) Modes adddress Safe Recovery Reliability -- differs from System Safety's analyses, which cover human safety*

Figure 3-2

Controversy exists concerning the tracking and aggregation of Category 1, and Category 2 failure modes with low probability of occurrence (Type E). Very few Critical Item List (CIL) issues (fewer than 10% of Cat-1 and Cat-2 failure modes) were reviewed at the Critical Design Review (CDR) as a result of this grouping strategy. The review team acknowledges that reviewing the Cat-1 and Cat-2 failure modes was not the sole purpose of the CDR. Nonetheless, the review team was concerned that the diminished visibility of these failure modes does not recognize the other uses of the CIL, such as formulating operating and maintenance procedures and mission rules. An independent observer at the SMA CDR noted: "If the current ground rules for Critical Items are continued, the X-33 Program management and NASA management will not be informed (have visibility) of all Loss of Vehicle/Death and Damage to Vehicle/Injury failure modes and interactions."

Resolution

In discussions concerning this issue at the on-site review LMSW indicated that Category 1 hazards or failure modes "will not slip through the crack". LMSW pointed to their computerized cross-referencing data base which identifies Critical Items on a system, sub-system, or component level for purposes of operations planning, maintenance, or other reasons. LMSW explained that the Cat-1 and Cat-2 failures get their own special attention, which includes quality acceptance and reliability centered maintenance. LMSW emphasized that they will not lose visibility of Category 1 items.

3.5 Fault Tree Analysis Process

The Fault Tree Analysis is one of the most powerful and widely used techniques of system safety on this program. Fault Tree Analyses were built and qualified for all critical X-33 components. There was evidence that probabilistic fault tree analyses were used to identify and rank critical failure combinations that lead to undesired outcomes. The technique was used to identify design changes in both hardware and software and to tailor operations and maintenance programs to eliminate or mitigate any additional issues identified downstream.

3.6 Range Safety Process

The Range Safety Process is under the control and direction of the United States Air Force, EAFB Commander. The Range Safety team also works with LMSW Flight Assurance and Operations groups. Flight Assurance chairs the Flight Working Group (FWG), to address issues regarding public safety and emergency preparedness. The Range Safety Office is responsible for all issues regarding Flight Termination System (FTS) design reliability and redundancy, as well as FTS command-destruct and communication system security. The Range Safety Launch Approval process is mapped in Figure 3.3 shown below.

The